UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,312	03/17/2005	Markus Franke	2002P15289WOUS	2692

7590 12/09/2009

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, NJ 08830

EXAMINER	
HAILU, TESHOME	
ART UNIT	PAPER NUMBER
2434	
MAIL DATE	DELIVERY MODE
12/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/528,312
Filing Date: March 17, 2005
Appellant(s): FRANKE ET AL.

Janet D. Hood
Reg. No. 61,142
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 09/02/2009 appealing from the Office action mailed 04/10/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0108042	Oka	08-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Oka (Oka) (US Pub. No. 2002/0108042).

As per claim 6 Oka discloses:

A method for generating and/or validating electronic signatures, the method comprising: (page 3, paragraph 31, certificate authority may have a verification key database which stores keys for signature verification in association with each of the plurality of signature modules; and the certificate authority may verify signatures by each of the plurality of signature modules).

Generating an asymmetrical key pair which includes a private signature key and a public validation key; (page 2, paragraph 13, the certificate authority also generates public and private keys as needed).

Calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function; (page 1, paragraph 9, the user A also attaches

signatures to the documents using the private key. The indefinite number of users goes through the predetermined procedure to obtain the public key from the public key certificate and have the attached signatures verified).

Performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid signature. (page 12, paragraph 193, fig. 22 shows an example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA1) 311. Numerals (1) through (10) in FIG. 22 represent steps to be taken by the parties involved. These steps are described below in ascending order). Also see paragraph 193-203 and fig. 22. According to the steps on fig. 22, the signature verified (step 8) before the certificate is issued (step 9).

Claim 18 is rejected under the same reason set forth in rejection of claim 6:

As per claim 8 Oka discloses:

The method according to Claim 6, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key. (page 1, paragraph 11, A typical public key certificate shown in FIG. 1 includes: a certificate version number; a serial number allocated to a certificate user by a certificate authority (CA); algorithm and parameters used for signature by the RSA, ECDSA, etc.; a certificate authority name; the period of certificate validity; the certificate user's name (user ID); the user's public key; and a digital signature).

Claim 20 is rejected under the same reason set forth in rejection of claim 8:

As per claim 10 Oka discloses:

The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document. (Page 1, paragraph 12, a hash value is generated

using hash function, and the certificate authority's private key is applied to the hash value to generate the signature). Also see fig. 1.

Claim 22 is rejected under the same reason set forth in rejection of claim 10:

As per claim 12 Oka discloses:

The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document. (Page 13, paragraphs 201-203, the CA server 321 retrieves a verification key from the verification key database to check whether the signature on the received public key certificate is valid. If the signature is judged valid, the CA server 321 sends the signed public key certificate to the requesting registration authority (RA1) 311. In turn, the registration authority (RA1) 311 forwards the signed public key certificate received to the requesting end entity (EE) 300).

Claims 14, 16, and 23 are rejected under the same reason set forth in rejection of claim 12:

(10) Response to Argument

With respect to 35 U.S.C. 102(b) rejection of **claims 6 and 18** appellant argued that the art on record, Oka (US Pub. No. 2002/0108042), fails to teach the claim limitation "performing a certification of the public validation key wherein, when validation, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid". Examiner would point out that, Oka teaches this limitation as, (page 12, paragraph 193, fig. 22 shows an example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA1) 311. Numerals (1) through (10) in FIG. 22 represent steps to be taken by the parties involved. These steps are described below in ascending order). Also see paragraph 193-203 and fig. 22. According to the steps on fig. 22, the

signature verified (step 8) before the certificate is issued (step 9). According to Oka, the end entity (EE) sends the public key certification issuance request to certificate authority server through registration authority. Then the certificate authority execute signature using hardware security module (HSM). The CA check whether the signature is valid or not and then if it is judged valid, the CA sends the public key certificate to end entity (EE) through registration authority. Here validating the signature by CA takes place before certifying the public key. Once the signature is valid, the CA sends the public key certificate to end entity (meaning first generating signature and then certifying the public key). Also see paragraph 193-203 and fig. 22. According to the steps on fig. 22, the signature verified (step 8) before the certificate is issued (step 9). Also Oka clearly disclosed that the steps on fig. 22 are occurred in ascending order and since step 6 (generating signature) is occurred before step 9 (issuing certificate), Oka disclosed that "***only*** those signatures generated at a time prior to the certification of the public validation key are recognized as valid".

Appellant also argued that Oka fails to teach the claim limitation, "calculating an electronic signature for an ***electronic document*** by means of the private signature key" of claims 6 and 18. Also mentioned that the art on record teach only a signature for a certificate and doesn't teach a signature on a document. Examiner respectfully disagrees on this matter and would point out that, Oka teaches this limitation as, (page 1, paragraph 9, the user A also ***attaches signatures to the documents using the private key***. The indefinite number of users goes through the predetermined procedure to obtain the public key from the public key certificate and have the attached signatures verified).

With respect to 35 U.S.C. 102(b) rejection of **claims 8 and 20** appellant argued that the art on record, Oka (US Pub. No. 2002/0108042), fails to teach the claim limitation, "when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key". Examiner would point out that, Oka teaches this limitation as, (page 1, paragraph 11, A typical public key certificate shown in FIG. 1 includes: a certificate version number; a serial number allocated to a certificate user by a certificate authority (CA); algorithm and parameters used for signature by the RSA, ECDSA, etc.; a certificate authority name; the period of certificate validity; the certificate

user's name (user ID); the user's public key; and a digital signature). Examiner respectfully disagrees on this matter and would point out that the broad but reasonable interpretation of the claim language, "reference to the electronic document", could be any of the cited number (version number, serial number, authority name, user name or ID) in paragraph 11 of Oka as indicated in the rejection.

With respect to 35 U.S.C. 102(b) rejection of **claims 10 and 22** appellant argued that the art on record, Oka (US Pub. No. 2002/0108042), fails to teach the use of a hash value for the document. Examiner would point out that, Oka teaches this limitation as, (page 1, paragraph 12, the digital signature is generated to attest the whole range of certified items: certificate version number, certificate authority serial number, signature algorithm and parameters, certificate authority name, certificate validity, user ID, and user's public key. Illustratively, a hash value is generated using hash function, and the certificate authority's private key is applied to the hash value to generate the signature) and (page 1, paragraph 9, the user A also ***attaches signatures to the documents using the private key***. The indefinite number of users goes through the predetermined procedure to obtain the public key from the public key certificate and have the attached signatures verified). According to Oka, clearly disclosed that the hash value is generated and the private key is applied to the hash in order to generate the signature. Then the generated signature is attached to the document.

With respect to 35 U.S.C. 102(b) rejection of **claims 12, 14, 16 and 23** appellant argued that the art on record, Oka (US Pub. No. 2002/0108042), fails to teach the claim limitation, "a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document". Examiner respectfully disagrees on this matter and would point out that, Oka teaches this limitation as, (page 13, paragraphs 201-203, the CA server 321 retrieves a verification key from the verification key database to check whether the signature on the received public key certificate is valid. If the signature is judged valid, the CA server 321 sends the signed public key certificate to the requesting registration authority (RA1) 311. In turn, the registration authority (RA1) 311 forwards the signed public key certificate received to the requesting end entity (EE) 300). Appellant

argued that the art on record teach that the certificate authority (not the author) checks the validation. However, checking the validation using the certificate authority (automatically) or author (manually) doesn't make any different. Also for clarity purpose, examiner would point out that making a manual activity automatically doesn't make any difference as long as it produces the same end result. See MPEP 2144.04(III).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Teshome Hailu/

Examiner, Art Unit 2434

Conferees:

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

/Christian LaForgia/
Primary Examiner, Art Unit 2439